Statement of

J. Brent Williams

Chief Technology Officer, Anakam, Inc.

before the

Health Information Technology Policy Committee

Authentication Workgroup

January 7, 2010

Statement of J. Brent Williams

Chief Technology Officer

Anakam, Inc.

HIT Policy Committee Authentication Workgroup

January 7, 2010

Dr. Lanksy, Mr. Weitzner, and members of the workgroup, thank you for the opportunity to provide our testimony on authentication solutions available for the healthcare industry. As the Chief Technology Officer of Anakam, Inc., I am pleased to provide our perspectives on the successful implementation of authentication across a broad healthcare information trust fabric.

Anakam understands that the healthcare information trust fabric will be bound together by a variety of authentication technologies and solutions. Each of these should be employed in a risk-adjusted framework that is considerate of the usability of the solution, the sensitivity information being protected, the cost of the technology and impact on the underlying business processes, and the context of the access. Fundamental to our view of this architecture is that organizations can only establish trust between one-another after they have established trust with their end users, their own systems, and the other organizations with whom they interface – hence why this is a complex fabric of trust. While this trust is established by a very wide variety of tools in the information technology lifecycle, authentication provides visibility into the risk presented by the actual end users of the systems. Once a level of trust or confidence can be associated with the identity end users across the user base, much of the other elements of functionality, access control, disaster recovery, remote access, etc can be established with far greater confidence.

The following section answers the specific questions directed at Anakam.

<u>Question #1: What trust problems are you trying to solve and for what range of users (e.g. organizations, individuals, health care professionals, consumers)? Please provide some quantitative data if possible to characterize your user base (e.g., percentage or number of each type).</u>

The Anakam Identity Suite® is designed to solve authentication challenges associated with extremely large, heterogeneous populations of users, who require secure access to sensitive data and systems.

User populations in the healthcare system have many different characteristics. There are internal users, who may be good candidates for company-issued computer equipment or authentication devices like cards or tokens, and other users, who are external to the enterprise but still need secure access to systems or data. Some users access systems daily or even hourly, and others access infrequently or

episodically. Some individuals are well known to the enterprise because they have done in-person business there for years (e.g., long-term patients of a medical practice) or because they have undergone in-person identity verification (e.g., physicians admitted to practice in a hospital), and some individuals are not known because they are new or because they have never conducted business in person (e.g., individuals who set up online Personal Health Records). The Anakam platform was designed specifically to address the challenges of organizations that deal with such populations. It is an integrated software platform that enables multiple authentication vectors and a secure registration process for strong authentication credentials. Anakam's software is generally installed inside the enterprise alongside the existing enterprise access management and identity management tools. More recently, some of our customers have decided to host our software for other entities, providing Identity as a Service (IaaS) in a cloud-based environment.

Anakam.TFA® Two-Factor Authentication is our flagship product that enables strong, two-factor authentication (NIST Level 3) without the expense or complexity of managing hardware or software tokens. We have used the basic paradigm of "something you know plus something you have," but instead of having the "something you have" issued by the enterprise, we enable users to register devices they already have. Instead of having to carry around cards or tokens, or having to download software to a specific device, we allow users to register devices they already have and use for other purposes, including cell phones or home or office phones. For those occasions when users need to retrieve their second-factor passcode from any phone, we provide them with the ability to register a voice biometric signature. The login process is completely intuitive: the user enters first factor credentials, as usual, retrieves the second factor passcode from the pre-registered device, enters that passcode, and proceeds with the transaction.

What end users do not see is that the behavior of second-factor challenge is risk-based. We have enabled enterprises to build their deployments around risk factors like geolocation, transaction frequency, device ID, and other indicators of risk. We have also enabled enterprises to provide a range of second-factor challenge modalities to allow them to minimize disruption to end users and match authentication challenges to the level of user sophistication and transaction risk.

As we entered the market, it became clear that with our two-factor authentication solution in place, our customers now had the challenge of registering and validating the identity claims of the large numbers of users who would sign up for authentication. We, therefore, incorporated remote identity proofing and verification into our software platform so that individuals can have their identity validated in real time, register for two-factor authentication credentials, and begin using those credentials immediately. Again, this is all done within a defined risk envelope. In some cases, remote identity proofing is all that is necessary for full access to systems and data; in other cases, depending on sensitivity of the transaction and the risk profile presented by an identity, additional proofing may be required.

As our customers learned more about our solution, some of them decided to implement it not only on their patient-facing applications, but also in practitioner-facing applications. To enable this, we added a capability to check an individual's professional credentials and tie that information to the strong authentication credential. A most interesting paradigm shift in this market is the clear move from the

use of the practitioner's credentials by all staff in an office to the ability to cost-effectively distribute appropriate credentials to various members of the staff and modify workflows so that each member of staff performs appropriate functions in a way that provides valid audit trails and non-repudiation. For example, non-prescribers may have key roles in the e-prescribing process before the practitioner with prescribing authority actually "signs-off" on the prescription, and with Anakam credentials this can be done so that the identity of each individual in the process is unambiguously recorded. Now, when they issue remote access credentials, our customers can determine whether the person applying for remote access is a practitioner licensed to practice in the state or a member of office staff affiliated with a particular practice. Anakam's software then feeds the access manager with rich information upon which to make decisions driving access controls and authorizations such that the end users are provisioned appropriately.

Anakam has multiple tens of millions of end user licenses sold across our customer base. Our customer base spans healthcare, government, banking, and ecommerce companies. Within healthcare, we segment the market based upon the end users of our authentication solutions: Providers and Hospitals, Patients and Caregivers, Exchanges and Networks, Payors, and ePrescribers. Because this is the way we view the market, there is frequently an overlap wherein we have federal or state government clients that are also healthcare clients. We have clients across all segments of the healthcare space at varying levels of adoption. Health information exchanges (HIEs) and regional health information organizations (RHIOs) were early adopters, hosting Anakam's software for their own patient and provider Web authentication to EHR or PHR functionality as well as to general patient portals. These early adopters have in some cases transformed themselves to provide Anakam as a service so that other HIEs and RHIOs in their states or regions can benefit from their efforts. Hospital systems and provider organizations became the next customer base to adopt Anakam's solution. These organizations adopted Anakam predominantly to provide remote authentication for patients into PHRs via the Web; however, many of the existing clients are migrating their remote employee authentication needs to Anakam for virtual private network authentication. ePrescribing networks became the next adopter. ePrescribers seek a solution to provide strong authentication for providers and provider staff for Web-based ePrescribing. Organizations that provide prescription information to patients via their PHRs are also adopting Anakam's identity proofing and authentication technologies to mitigate risks associated with providing this data to people with whom they may not have a direct or face-to-face relationship.

<u>Question #2: Who pays for the solution, implementation, processes and support for your approach? What factors contribute to the total cost of ownership of the technologies, including process costs? What are the implications to widespread deployment?</u>

Anakam's enterprise customers pay for the Anakam software. Anakam's strong authentication software layers sits alongside the traditional first factor (username/password) authentication solutions within the enterprise. It is this combination that provides the NIST SP 800-63 Level 3 authentication when required or may be adapted to other forms of risk-based authentication based upon the needs of the enterprise. Typically, when Anakam is implemented, the enterprise will have already selected an access management strategy. This could be an enterprise-wide strategy where everybody authenticates through one or more large scale access management products common-place in the industry.

Alternatively, within the healthcare industry, we have been implemented along side of core business applications like EHRs and PHRs with their intrinsic username/password management system. It is rare that an enterprise must separately procure the access management strategy, and within the healthcare industry, it has only occurred in "greenfield" HIE or RHIO implementations where the enterprise identity strategy had yet to be determined.

When working with a large hospital or enterprise with numerous business applications, we frequently find the Anakam software layered on top of an access management tool that has been implemented in parallel with a single-sign-on (SSO) tool such that the enterprise authentication platform can provide enterprise-wide authentication. If that hospital or enterprise has also undertaken a federated identity strategy, Anakam provides the strong authentication supplement on top of the federated access manager also.

Since Anakam developed our product set for the mass scale marketplace, total cost of ownership was critical to providing a cost effective solution for our customers. First, our goal was to provide a solution in a market where a solution was not previously established. Anakam customers recognized an immediate net positive TCO simply through the implementation of an appropriate privacy protection solution that offered Anakam clients the ability to offer new services online that had been unavailable due to the lack of consumer-facing strong authentication. They were able to shift paper-based, manual processes to Web-based transactions that removed the costs of paper processing and telephone-based solutions and improved customer service and quality of service at the same time. Infrastructure requirements for telecommunications and network capacity vary based upon the risk thresholds and enterprise risk management practices. Best practices show that a risk based solution leverages less costly, non-telecom dependent solutions for lower risk transactions and increases the authentication strength and need for alternate communications channels that provide the "out-of-band" connectivity for strong two-factor authentication in higher risk scenarios. End-users may also participate in the cost of the transaction because they may have to pay for transactional services used for the authentication method depending upon the modes used and the frequency of access.

Since Anakam looks at the solution from a comprehensive lifecycle management point of view, we also found that the implementation of Anakam's identity proofing platform provides a positive TCO for our customers. The process of identity proofing using face-to-face or remote telephonic transactions is far more expensive than introducing web-based dynamic knowledge-based authentication. As part of our focus on TCO and ease of use, we chose not to develop a new platform for a marketplace that already has a large number of solutions. Instead, we developed an interface layer that greatly simplifies the customer interface process, requiring the customer to only interface with the Anakam platform, and Anakam manages the interfaces with various knowledge-based authentication providers in the market, tailoring the solution to meet our customers' need and supporting the automated provisioning of the underlying access management solution and Anakam.TFA at the same time.

The best part of widespread deployment is the fact that end users will not have large number of cards and tokens around their necks, in their wallets and purses, or on their key chains. Instead, since Anakam's technology provides token equivalent authentication using devices they already have, end-

user management and adoption is greatly simplified. End users will still have access cards and tokens for those limited environments where they have physical access control requirements like clinical environments or government office buildings, and they will still use these credentials to perform sensitive electronic transactions such a workstation login or local encryption with a private key…none of which are possible with Anakam, but their use cases are limited to within the enterprise. Anakam's value become apparent outside of the enterprise or across enterprises where a user will have numerous credentials and the need for strong credentials to enable new trusted, cost-efficient, and customer friendly business practices online is critical.

Question #3: Directory services often support some certificate authority or other authentication mechanism. As you look more broadly at the architecture, how do your approaches work with such directory services?

Anakam is independent of the directory services infrastructure. An enterprise can implement everything from a standards-based LDAP implementation to a custom relational directory of users, passwords, and access controls. Further, Anakam works with any certificate provider. We are simply a software product that interfaces to existing authentication tools to provide the strong authentication. If an enterprise is currently using a username password solution to release a digital certificate, they can modify that process to add Anakam's progressive, risk-based multi-factor solution to augment the process.

As we look more broadly at the directory and certificate solutions in the marketplace, we recognize that about the most important issue is finding a workable solution to create the healthcare identity trust fabric. This fabric needs to allow for localized trust establishment and enrollment of those with strong privileges and access rights, like practitioners and staff, as well as those with lesser privileges and access rights, like patients and caregivers.

Fundamental to understanding the next generation of identity solutions is the need to clear up three great misconceptions that we have seen prevalent in the healthcare industry:

- Misconception 1 – *Federated identity will allow a practitioner in one enterprise to search for information on a patient and get information out of multiple systems*. There is general confusion about the difference between federated identity and federated search. Federated identity would allow a practitioner to log in to a "home" system and search for patient data in that system. Federated identity would allow him or her to click on a link to gain access to another system which would accept the federated identity credentials from the "home" system and search in that system, and then repeat for another system, and another, and another – each of the systems accepting the federated identity, but not searching in a federated manner. **Reality**: Practitioners want to be able to login in on one platform and search for patient information by initiating one query and having that query return information from numerous locations. This process is actually federated search, not federated identity.
- Misconception 2 – *A practitioner logs into the hospital identity management system. The same practitioner asserts their identity into another hospital's application using federation and then*

has special identity-based permissions unique to their name. To accomplish this, the practitioner is enrolled in the hospital's federated identity management system and then has a separate enrollment in the other hospital's application to provide additional certifications that justify their access to the other data. **Reality**: The benefits of federated identity no longer exist when a user is enrolled in both the federated identity application and the consuming application. The concept of federation is that the consuming system does not have to enroll the user and instead accepts the federated identity provider's assertion of identity. If the user exists in both directories, then federation is actually replaced by single-sign-on wherein the federated identity manager is providing the authentication and then asserts the identity and the user is still enrolled.

- Misconception 3 – *PKI is Authentication*. Yes, PKI provides a mechanism for communicating authentication…or authenticity of a claim. It allows an end-user or system to ascertain the validity of an assertion using cryptographic processes. **Reality**: PKI is an elegant solution overcome by the complexity of the credential. PKI is only as good as the authentication process. An enterprise can implement an iron-clad PKI solution with expensive certificates yet still release those certificates with a simple username and password.

Question #4: Does your approach support a delegated authentication model where there is an authorized registrar that issues the authentication credentials to individuals? If so, how? Are there implications for interoperability in this scenario?

Critical to this discussion is understanding delegation in the identity management lifecycle. Within the context we are addressing here, we look at the identity management lifecycle as a series of steps:

- Registration and Enrollment – the process of gathering the biographic information (and biometric information if applicable) about an individual
- Identity Proofing – the process of validating the association of the asserted biographic information with the actual individual
- Professional Credentialing – the process of associating the professional credentials of an individual (if required) with the individual's identity and with the electronic credentials
- Issuance – the process of providing associating the logical credentials of an individual with their actual identity
- Authentication – the ongoing use of the credentials to assert the identity of an individual
- Authorization – the provisioning of an individual with access to certain business functions and data based upon their identity, role, location, credentials, or status
- Access Control – the control of access to applications and data based upon the authentication and authorization
- Change Management – the updating, including removal, of the credentials for an individual

Delegation can take place in various parts of the identity management lifecycle. Delegation of identity proofing and credentialing is radically different than delegation of authentication. Within the healthcare trust fabric, we may delegate identity proofing and credentialing to a local representative for highly sensitive transactions or sensitive information of multiple individuals, but at the same time, we may

accept self-assertion of identity or remote identity proofing and verification for less sensitive transactions. Delegation of authentication is a radically different story. Delegation of authentication can take place by an enterprise that accepts federated identity credentials from external parties – which also means that they accept delegation of identity proofing. Additionally, delegation of authentication can occur when one application allows another application to conduct the access management transaction on its behalf and trust the access management decision through a single-sign-on token exchange.

In the end, the healthcare trust fabric needs to leverage delegation of identity proofing, professional credentialing, and authentication as part of a comprehensive approach to risk management. Whether the healthcare industry uses PKI or SAML or any other solution to provide remote assertion of identity proofing and authentication across the fabric, the complexity does not lie in the technology, instead it lies in the complex business rules and agreements that govern identity-related trust. These rules have been established by NIST for the federal government. Several commercial standards groups, including Kantara, OpenID, and Information Card, are attempting to implement similar standards across the commercial industry. Anakam's recommended approach for adopting these standards is detailed in the answer for question 5, below.

Question #5: What should be the role of government? Where can rapid action address common concerns or limitations of trust?

Anakam believes the government has a key role in the authentication process. This role can take the form of a plan of action.

- To facilitate rapid action, the government should establish a policy framework, tied to a set of standards, requirements, guidelines, and capabilities for identity management. An example of such a framework for the federal government is the Office of Management and Budget Memorandum M-04-04, which defined four levels of identity assurance for federal transactions. However, examples and technologies associated with the policy framework need to be sufficiently flexible to allow for changes in the risk environment, needs of emerging business applications, and responses to evolving threats.
- The federal government should establish minimum required identity verification and authentication standards based upon simple, clear, and understandable rules, such as those in NIST SP 800-63-1. Further, the government should continue to encourage the use of risk analysis (as required by HIPAA) for the management of instances above and beyond the minimum.
- State governments should continue to maintain responsibility for identifying special categories of sensitive health information including reproductive health, behavioral health, or minors' health. State governments should leverage the federal requirements and define what further requirements exist and how they relate to authentication that provides access to special categories of information within the state.
- The federal government should establish the National Electronic Healthcare Identity Strategy. Anakam has provided a description of such a strategy to HHS ONC. Under our proposal, patients

would be able to opt-in to a unified identity management system that allows a unique identifier that enables convenience of nation-wide acceptance and record linkage when a patient wants it. At the same time, patients who do not want the convenience of single unified identity would have the option of enrolling unique identities across numerous providers. Providers are already required to have a unique identifier. The federal government and larger institutions would establish solutions that federate patient and provider identities under a common federation agreement that established accepted identity proofing and authentication requirements. Smaller institutions would be able to deploy their own solutions that federate at the national level or subscribe to solutions hosted by large institutions or to HIE/RHIO solutions.